UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NOTICE OF PROPOSED RULEMAKING	**)**	**Docket No. RM06-22-000**
	)	
MANDATORY RELIABILITY STANDARDS FOR	**)**	
CRITICAL INFRASTRUCTURE PROTECTION	**)**	

COMMENTS OF

REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY
REP. PETER T. KING (R-NY), RANKING MEMBER,
COMMITTEE ON HOMELAND SECURITY

REP. JAMES R. LANGEVIN (D-RI), CHAIRMAN, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY
REP. MICHAEL T. MCCAUL (R-TX), RANKING MEMBER, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY

REP. SHEILA JACKSON-LEE (D-TX), CHAIRMAN,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
REP. DANIEL E. LUNGREN (R-CA), RANKING MEMBER,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

ON THE NOTICE OF PROPOSED RULEMAKING FOR MANDATORY RELIABILITY STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION

October 5, 2007

TABLE OF CONTENTS

UNITED STATES OF AMERICA
BEFORE THE
FEDERAL ENERGY REGULATORY COMMISSION

NOTICE OF PROPOSED RULEMAKING	**)**	**Docket No. RM06-22-000**
	)	
MANDATORY RELIABILITY STANDARDS FOR	**)**	
CRITICAL INFRASTRUCTURE PROTECTION	**)**	

COMMENTS OF

REP. BENNIE G. THOMPSON (D-MS), CHAIRMAN,
COMMITTEE ON HOMELAND SECURITY
REP. PETER T. KING (R-NY), RANKING MEMBER,
COMMITTEE ON HOMELAND SECURITY

REP. JAMES R. LANGEVIN (D-RI), CHAIRMAN, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY
REP. MICHAEL T. MCCAUL (R-TX), RANKING MEMBER, SUBCOMMITTEE ON
EMERGING THREATS, CYBERSECURITY, SCIENCE AND TECHNOLOGY

REP. SHEILA JACKSON-LEE (D-TX), CHAIRMAN,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION
REP. DANIEL E. LUNGREN (R-CA), RANKING MEMBER,
SUBCOMMITTEE ON TRANSPORTATION SECURITY AND INFRASTRUCTURE PROTECTION

ON THE NOTICE OF PROPOSED RULEMAKING FOR MANDATORY RELIABILITY STANDARDS FOR CRITICAL INFRASTRUCTURE PROTECTION

I. INTRODUCTION

As Members of Congress, we are pleased to provide these comments in response to the Notice of Proposed Rulemaking ("NOPR") issued in the above-captioned docket.[1] We support the efforts of the Federal Energy Regulatory Commission ("FERC") to require the North American Electric Reliability Corporation ("NERC") to develop modifications to the Critical Infrastructure Protection ("CIP") Reliability Standards. However, we believe that the reliability of the nation's bulk-power system ("BPS") will be better protected by a cybersecurity standard that incorporates the additional security measures of National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-53 as applied to industrial control systems.

[1] Notice of Proposed Rulemaking: Mandatory Reliability Standards for Critical Infrastructure Protection (Docket No. RM06-22-000), issued July 20, 2007.

II. NOTICES AND COMMUNICATIONS

Notices and communications with respect to this filing may be addressed to:

Jacob Olcott
Subcommittee Director and Counsel
Emerging Threats, Cybersecurity,
Science and Technology Subcommittee
Committee on Homeland Security
U.S. House of Representatives
H2-176 Ford House Office Building
Washington, D.C. 20515
(202) 226-2616
(202) 226-4499 (facsimile)
Jacob.Olcott@mail.house.gov

III. BACKGROUND

The BPS of the United States and Canada has more than $1 trillion in asset value, more than 200,000 miles of transmission lines, and more than 800,000 megawatts of generating capability serving over 300 million people.[2] The effective functioning of this infrastructure is highly dependent on control systems, computer-based systems that are used to monitor and control sensitive processes and physical functions. Once largely proprietary, closed-systems, control systems are becoming increasingly connected to open networks, such as corporate intranets and the Internet. According to the United States Computer Emergency Readiness Team ("US-CERT"), "this transition towards widely used technologies and open connectivity exposes control systems to the ever-present cyber risks that exist in the information technology world in addition to control system specific risks."[3]

The cyber risk to these systems is becoming increasingly dangerous. Ten years ago, the President's Commission on Critical Infrastructure Protection ("PCCIP") released a report on the risks associated with interconnected computer systems on the BPS, stating that "the widespread and increasing use of supervisory control and data acquisition systems for control of energy systems provides increasing ability to cause serious damage and disruption by cyber means."[4] Since the release of that study, numerous unintentional cyber incidents – from the Davis-Besse power plant incident in 2003, to the Northeast blackout, to the Browns Ferry nuclear power plant failure in 2006 – suggest that the concerns raised by the PCCIP were warranted.

---

[2] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Multiple Efforts to Secure Control Systems Are Under Way, but Challenges Remain* (October 2007), p. 27.
[3] U.S. Department of Homeland Security, Control System Security Program Fact Sheet, available at http://www.us-cert.gov/control_systems/pdf/CSSP_FactSheet_sml.pdf.
[4] U.S. Government Accountability Office, Report to Congressional Requesters, *Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems* (March 2004), p. 2.

But nothing quantified the intentional threat to the BPS quite like the experiment performed by the Idaho National Laboratory for the Department of Homeland Security. In September 2007, the Department disclosed that its researchers successfully destroyed a generator while conducting an experimental cyber attack. According to news reports, the attack involved a controlled hack of a replicated control system commonly found throughout the BPS.[5] The results of this experiment suggest that malicious actors could use the same attack vector against larger generators and other critical rotating equipment that could cause widespread and long-term damage to the electric infrastructure.

Clearly, intentional and unintentional control system failures on the BPS can have a significant and potentially devastating impact on the economy, public health, and national security of the U.S. For a society that runs on power, the discontinuity of electricity to chemical plants, banks, refineries, hospitals, water systems, and military installations presents a terrifying scenario. Economists recently suggested that the loss of power to a third of the country for three months would result in losses of over $700 billion.[6] This figure does not consider the negative societal or health ramifications that such an event would have on the American people.

The FERC proposes to approve a set of reliability standards to help safeguard the nation's BPS against potential disruptions from cyber attacks. The proposed standards require certain users, owners and operators of the grid to establish plans, protocols and controls to safeguard physical and electronic access to systems, to train personnel on security matters, to report security incidents, and to be prepared to recover information. The FERC recently created an Office of Electric Reliability ("OER") designed to focus on the development and implementation of these standards for the users, owners, and operators of the grid.

Unfortunately, we believe the standards proposed by the NERC for adoption by the FERC do not sufficiently ensure the production or delivery of power in the event of intentional or unintentional cyber incidents involving critical infrastructures. We are primarily concerned with five issues: 1) the limitations of CIP-002-1 which exclude critical assets from the risk methodology; 2) the failure of the NOPR to consider the dependencies of critical infrastructures on the BPS; 3) the absence of clearly defined characteristics that will comprise a risk methodology; 4) the interconnectivity of industrial control system data networks; and 5) the vulnerabilities created by using a separate standard for publicly- and privately-owned infrastructures. The fact that our comments are primarily related to the first of the proposed eight standards should not be construed as support of the remaining standards, but demonstrate our deep concern with the implementation of CIP-002-1. We believe that the reliability of the nation's BPS would be better protected by a cybersecurity standard that incorporates the additional

[5] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.
[6] (2007, Sept. 27). "Mouse click could plunge city into darkness, experts say," Retrieved Sept. 28, 2007, from http://www.cnn.com/2007/US/09/27/power.at.risk/index.html.

security measures of NIST Special Publication 800-53 as applied to industrial control systems.

IV. DISCUSSIONS OF MAJOR ISSUES OUTLINED IN THE NOPR

Though we applaud FERC's efforts and support many of its modifications to the NERC CIP Reliability Standards, we are primarily concerned with five issues: 1) the limitations of CIP-002-1 which exclude critical assets from the risk methodology; 2) the failure of the NOPR to consider the dependencies of critical infrastructures on the BPS; 3) the absence of clearly defined characteristics that will comprise a risk methodology; 4) the interconnectivity of industrial control system data networks; and 5) the vulnerabilities created by using a separate standard for publicly- and privately-owned infrastructures.

NERC's proposed CIP-002-1 requires an entity to identify its "critical assets" and "critical cyber assets" using a risk-based methodology. Identifying assets is arguably the most important step in the entire assessment process. With control systems becoming increasingly interconnected to each other, and also interconnected with corporate data networks and the Internet, many assets that were once thought to be isolated are now vulnerable.[7] As noted in the FERC Staff Preliminary Assessment, "because CIP-002-1 addresses the assessment methodology and process for identifying critical assets and critical cyber assets, it represents the critical first step that can fundamentally affect the chances for successful implementation of the remaining CIP Reliability Standards."[8] However, if implemented in its present form, CIP-002-1 would not require responsible entities to comprehensively secure "critical assets" that could in fact have a significant impact on the safety and security of the United States.

The problem lies with the NERC definitions of "critical assets." NERC defines "critical cyber assets" as "cyber assets essential to the reliable operation of critical assets."[9] "Critical assets" are defined as "facilities, systems, and equipment that would affect the reliability or operability of the BPS."[10] This is a conceptual mistake that fails to understand the importance of the reliability and operability of individual elements of the grid, which are essential to the delivery of power to the nation's critical infrastructure.

The BPS is an enormous, interconnected network that is both redundant and resilient, making the sole focus on "reliability" and "operability" of the grid as a whole inappropriate. Practically, there are several assets that would fall outside the scope of NERC's definition of "critical" which should not. For instance, although generation units

[7] Today, the existing "NERCnet" employed for inter-control center coordination arguably provides a direct link for hacker access to most utility control centers in North America.
[8] Federal Energy Regulatory Commission, *Staff Preliminary Assessment of the North American Electric Reliability Corporation's Proposed Mandatory Reliability Standards on Critical Infrastructure Protection*, December 11, 2006.
[9] North American Electric Reliability Corporation, Critical Infrastructure Protection Reliability Standard 002-1.
[10] North American Electric Reliability Corporation, Critical Infrastructure Protection Reliability Standard 002-1.

serving communities locally regularly trip offline due to both unexpected events and routine maintenance alike, service to customers generally remains constant. This is a credit to the design of the greater grid, which is engineered to withstand these kinds of singular events.[11] Critical to providing power for citizens, businesses, and other critical infrastructures, these units would not be defined as such because they would not affect the reliability or operability of the BPS itself. Similarly, individual substations may experience reliability problems, but unless the load shed exceeds a certain level of megawatts, it is unlikely that a single substation would be recognized as a critical asset under the NERC definition. Telecommunications equipment would also be excluded from the "critical cyber assets" list even though there are documented cases of computer worms denying service from control systems to substations.[12]

Finally, though it is impossible to argue that they are not critical to the safety and security of the U.S., distribution assets would be excluded because they are not essential to reliability of the BPS. Again, real world examples expose problems with this logic. Though the BPS was restored within days to the primary areas affected by Hurricane Katrina, it took some municipal water department pumps over a year to get back up and running because the distribution systems remained off-line. In a June 2007 incident, an outage in Tempe, Arizona, caused by the unexplained activation of the distribution load shedding program in the energy management system affected nearly 100,000 customers.[13]

It is easy to see that an intentional or unintentional cyber incident on the BPS resulting in the disability of any connected asset – from distribution control systems to telecommunications equipment – can have a significant impact on the nation's security. Every critical infrastructure in the country is dependent on the BPS: chemical plants, banks, refineries, hospitals, water systems, and military installations all rely on the effective operation in their region. Focusing on assets relative to the functioning of the grid as a whole misses the importance of each individual asset to the functioning of our society. Unfortunately, recognition of the major infrastructure dependencies on the BPS is entirely absent from the FERC NOPR. Though the NOPR suggests that FERC "will revisit this matter through future proceedings and with other agencies," it is difficult to understand why cross-sector dependencies on the BPS are not the main focus of this standards process.[14] To address this shortcoming, we suggest that every electronically connected asset be considered "critical," as failures on those systems could potentially cause cascading outages of the BPS that could affect every critical infrastructure associated with it.

---

[11] North American Electric Reliability Corporation, Transmission Planning Series Standards (TPL).
[12] On June 20, 2003, NERC issued a lessons learned advisory about the "SQL Slammer Worm," a computer worm that caused a denial of service on some Internet hosts and dramatically slowed down general Internet traffic in early 2003. However, CIP-002-1 excludes telecommunications equipment because it is not a "critical asset."
[13] U.S. Department of Energy, Office of Electricity and Delivery Reliability, Infrastructure Security and Energy Restoration, "Energy Assurance Daily" (June 29, 2007), available at http://www.oe.netl.doe.gov/docs/eads/ead062907.pdf.
[14] Notice of Proposed Rulemaking: Mandatory Reliability Standards for Critical Infrastructure Protection (Docket No. RM06-22-000), issued July 20, 2007.

We strongly support FERC's efforts to provide guidance on the content to be applied in the risk-based assessment methodology and require that a senior manager annually review and approve the methodology. We do hope, however, that FERC will create a meaningful deadline for the issuance of such guidance so that it can be effectively promoted across the system. It is true that one singular methodology is probably not appropriate for all situations or entities, but FERC should define the acceptable characteristics of a methodology. While flexibility is important, allowing each responsible entity to craft its own methodology may lead to difficulties in assessing risk across the system. Explicit requirements will avoid a situation where neighboring utilities with the same equipment can have completely different critical cyber assets by virtue of their interpretation of the definitions. Ultimately, however, as long as a responsible entity uses a risk-based methodology focusing on the reliability of the BPS rather than the critical infrastructure end user, safety and security concerns remain paramount. We expect FERC will establish an expedited timeline for responsible entities to complete their assessments and mitigation efforts.

V. CONCLUSIONS AND ACTIONS REQUESTED

The Energy Policy Act of 2005 created a statutory impediment on federal regulators seeking to enact higher standards of security on responsible entities operating within the BPS. We are concerned that the regulatory framework may lead to delays in the implementation of security standards that would better protect the BPS infrastructure and the critical infrastructures that depend on its operation. We endorse the FERC's interpretation of the Section 215 provision requiring "due weight" to be given to the technical expertise of the Electric Reliability Organization with respect to the content of a proposed standard without complete deference.[15] We believe that the FERC staff's technical expertise in control systems and cybersecurity and the proposals that they set forward in this rulemaking provide a valuable security perspective for the responsible entities charged with implementing these regulations.

A painful lesson from the September 11th attacks on our country is that a system is only as strong as its weakest link. On that day, several terrorists entered the U.S. transportation system through a small airport in Portland, Maine. Once inside the system, they were able to carry out their plans unimpeded. The Federal government must remain vigilant in eliminating weak links that can be exploited by those who wish to do us harm. In that vein, because of the interconnections between publicly- and privately-owned infrastructures that comprise the BPS, we believe that every responsible entity should be held to the same standards for securing their critical assets.

NIST is responsible for developing standards and guidelines, including minimum requirements, for providing adequate information security for all Federal agency non-national security operations and assets. In 2005, NIST released Special Publication (SP)

[15] Energy Policy Act of 2005, Pub. L. No. 109-58, Title XII, Subtitle A, 119 Stat. 594, Section 215(d)(5) (2005).

800-53, "Recommended Security Controls for Federal Information Systems." This publication was originally developed for use with traditional information technology systems. Recently, however, NIST established the Industrial Control System Security Project to improve the security of publicly- and privately-owned industrial control systems. The major focus of the project is to clarify and rectify problems experienced in applying SP 800-53 to industrial control systems and develop new requirements in those areas. In December 2006, NIST published SP 800-53 Revision-1 that provides interim guidance on the application of the security controls to industrial control systems. These specifications are binding on federal government agencies.

NIST research also focused on comparing the proposed NERC Reliability Standards for cybersecurity with SP 800-53. According to a NIST-sponsored review published in March 2007, an organization conforming to the baseline set of security controls in SP 800-53 will also comply with the management, operational and technical security requirements of the NERC Reliability Standards, though the converse may not be true. For instance, in the Tempe outage and SQL Slammer Worm incidents, the NERC Reliability Standards allow for the exclusions of telecommunications and distribution equipment from the "critical assets" list. Under the SP 800-53 requirements, however, there is no similar exclusion, and it is reasonable to conclude that a responsible entity could identify and mitigate vulnerabilities in these assets prior to an incident. The technical report concluded that the NERC Reliability Standards are both "inadequate for protecting critical national infrastructure," and "inadequate for all electric energy systems when the impact of regional and national power outages is considered."[16] In its February 2007 comments on the FERC Preliminary Staff Assessment, NIST researchers concurred, stating that the NERC standards "do not provide levels of protection commensurate with the mandatory minimum federal standards (FIPS) prescribed by NIST."[17]

Because of the interconnectivity between Federally- and privately-owned elements of the BPS, inconsistent regulatory structures create weak links and potential vulnerabilities in the entire system. A responsible entity in the private sector may fully implement the NERC Reliability Standards but will fall short of the security measures implemented by a public entity. According to a report by MITRE sponsored by NIST, "to date, there has been no serious effort to ensure that the cybersecurity standards and best practices emerging from the electric power industry are consistent with the federal standards and guidelines being developed by NIST in response to the FISMA."[18] We believe that this is a significant problem that must be addressed immediately. Though the NOPR specifically declines to propose that NERC incorporate any provisions of the NIST guidelines in the CIP Reliability Standards, in light of the security concerns at issue in this rulemaking, we urge the FERC to modify the standard so that it incorporates aspects of SP 800-53 and the related NIST standards.

---

[16] Marshall D. Abrams, "Addressing Industrial Control Systems in NIST Special Publication 800-53," MITRE Technical Report (March 2007), p. 2-20.

[17] Stuart Katzke and Keith Stouffer, *Comments on the FERC Staff Preliminary Assessment of the NERC Proposed Mandatory Reliability Standards on Critical Infrastructure Protection issued December 11, 2006 Docket RM06-22-000*, Feb. 6, 2007.

[18] Marshall D. Abrams, "Addressing Industrial Control Systems in NIST Special Publication 800-53," MITRE Technical Report (March 2007), p. 2-20.

In closing, we applaud FERC for proposing these regulations. We are hopeful that both FERC and NERC will find these comments helpful and incorporate them when finalizing their rules for cybersecurity.